UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH DAKOTA
SOUTHERN DIVISION

LODGENET INTERACTIVE CORPORATION, a Delaware corporation, Plaintiff, v. NOMADIX, INC., a Delaware corporation, Defendant.	Civil Action No. 10-cv-04036-RAL **[PROPOSED] PROTECTIVE ORDER**

The parties have filed a Joint Motion for a Protective Order (Doc. 42). For good cause, it is

ORDERED, pursuant to Fed. R. Civ. P. 26(c), that trade secret or other confidential information be disclosed only in designated ways:

1. As used in the Protective Order, these terms have the following meanings:

"Attorneys" means counsel of record;

"Confidential Documents" are Documents designated pursuant to paragraph 2;

"Confidential - Attorneys' Eyes Only Documents" are the subset of Confidential Documents designated pursuant to paragraph 5 as "Confidential - Attorneys' Eyes Only;"

"Highly Confidential – Source Code – Restricted Access Only Material" refers to the subset of Confidential Documents designated pursuant to paragraph 5 as "Highly Confidential – Source Code – Restricted Access Only;"

"Protected Technical Material" refers to (1) technical Confidential - Attorneys' Eyes Only Documents that describe the structure and/or operation of a Producing Party's product, including design documents, schematic diagrams, manufacturing drawings, engineering drawings, engineering notebooks, specifications, research notes and materials, and other technical descriptions and/or depictions, in whatever form such Documents exist; and (2) Highly Confidential – Source Code – Restricted Access Only Material;

"Documents" includes all materials within the scope of Fed. R. Civ. P. 34, exhibits, excerpts, summaries, pleadings, reports, declarations, affidavits, testimony, transcripts, interrogatory responses, admissions, or other discovery material and any copies thereof;

"Producing Party" refers to any party or non-party that provides one or more Documents;

"Receiving Party" refers to any party or non-party that receives, is shown, or is otherwise exposed to one or more Documents; and

"Written Assurance" means an executed document in the form attached as Exhibit A.

2. By identifying a Document "Confidential," a party may designate any Document, including interrogatory responses, other discovery responses, or transcripts, that it in good faith contends to constitute or contain trade secret or other confidential information.

3. All Confidential Documents, along with the information contained in the Documents, shall be used solely for the purpose of this action, and no person receiving such Documents shall, directly or indirectly, transfer, disclose, or communicate in any way the contents of the Documents to any person other than those specified in paragraph 4. Prohibited purposes include, but are not limited to, use for competitive purposes or the prosecution of additional intellectual property rights. Any individual (including a party's attorneys) to whom any Protected Technical Material has been disclosed that was produced by another party or non-party and that has not lost its confidential status, shall not thereafter, until two (2) calendar years after the termination of this action (including any appeals), on behalf of a patent applicant or patentee, prepare and/or amend any patent applications of any kind, draft and/or amend patent claims of any kind (including claims that are the subject of reissue or reexamination proceedings), supervise such activities, or consult on such activities whenever such patent applications or patent claims relate to (1) the patents-in-suit or contain claims that it is reasonably likely may be asserted against the Producing Party in this action or any other action; and relate to (2) charging for, providing or controlling access to computer networks, or to network devices involved in charging for, providing or controlling access to computer networks. Attorneys to whom Protected Technical Material has been disclosed may provide patent prosecution counsel with public information produced in this action so that the information may be filed with the U.S. Patent Office. This paragraph shall not restrict consultation regarding strictly procedural or legal aspects of patent prosecution (including reissue or reexamination proceedings) that do not involve the merits, substance or

technical nature of the patent prosecution. This paragraph shall also not restrict consultation regarding, or other involvement in, the preparation of arguments regarding prior art or patentability over prior art (including when such arguments are made in connection with reissue or reexamination proceedings).

4. Access to any Confidential Document shall be limited to:

(a) the Court and personnel of the Court;

(b) a party's outside law firm and the law firm's law clerks, paralegals, secretaries, clerical staff, and other persons regularly employed by such law firm, and any temporary personnel retained by such law firm to perform legal or clerical duties or to provide logistical litigation support reasonably necessary to assist in the law firm's conduct, including service contractors (such as document copy services);

(c) persons shown on the face of the Document to have authored or received it;

(d) any interpreter, court or short hand reporters, or typists retained to translate, record, or transcribe testimony;

(e) these inside counsel: FOR PLAINTIFF: James Naro, LodgeNet Interactive Corporation; FOR DEFENDANT: Mr. Kelly Hughes, Nomadix, Inc.;

(f) outside independent persons (i.e., persons not currently or formerly employed by, consulting with, or otherwise associated with any party) who are retained by a party or its attorneys to furnish technical, consulting, or expert services (together with their associates and clerical staff whose duties and responsibilities require access to Confidential Documents), or to provide assistance as mock jurors, jury or trial consultants, or focus group members or the like, and/or to give testimony in this action;

(g) jurors serving in any trial of this action; and

(h) any other person agreed to by the Producing Party in writing.

5. The parties shall have the right to further designate Confidential Documents or portions of Documents as "Confidential - Attorneys' Eyes Only." The parties shall also have the right to designate Confidential Documents or portions of Documents which are descriptive of computer-based algorithms used in a Producing Party's product, including software source code, as "Highly Confidential – Source Code – Restricted Access Only." Disclosure of Documents designated "Confidential - Attorneys' Eyes Only" or "Highly Confidential – Source Code – Restricted Access Only," or the information contained therein, shall be limited to the persons designated in paragraphs 4(a), (b), (c), (d) and (f). Persons in paragraph 4(f) may have access to Documents or portions of Documents designated "Confidential - Attorneys' Eyes Only" or "Highly Confidential – Source Code – Restricted Access Only," or the information contained therein, only to the extent allowed by paragraph 7.

a. For software source code and files related to source code (e.g., configuration files, Makefiles, files storing input or output related to source code and/or the program that the source code underlies, files related to source code management and/or revision systems, read me files, etc.) that are to be produced:

i. The Producing Party shall produce the source code and all related files in native format and broken out by version number and, if applicable, product name and/or product model number. The Producing Party shall identify or supply software and/or programming tools that can be used to view and compile the source code.

ii. The production of a given version of source code and related files shall preserve all file names, directory names and directory structures.

iii. The Producing Party may produce source code and related files designated "Highly Confidential – Source Code – Restricted Access Only" pursuant to this Protective Order on an encrypted CD(s), DVD(s), hard drive(s), virtual drive(s) or other media.

iv. To the extent that total compliance with subparagraphs (i) and (ii) would be infeasible or burdensome for a Producing Party with respect to non-source-code Documents or information (e.g., with respect to source code management or revision system files), the Producing Party and Receiving Party will discuss solutions wherein the Documents or information are produced electronically and reasonably in compliance with subparagraphs (i) and (ii). This subparagraph (iv) does not exempt production of source code from compliance with subparagraphs (i) and (ii).

v. Subparagraphs (i) through (iv) apply to the extent the source-code Document or file related to source code is available to the Producing Party in native format. If the Document is not available in native format (because, e.g., it is a printout of source code with handwritten remarks), the Document may be produced in accordance with the parties' agreements regarding other types of Documents.

b. To the extent any Receiving Party (apart from the persons identified in paragraph 4(a)) electronically maintains Highly Confidential – Source Code – Restricted Access Only Material, such Receiving Party shall maintain such Highly Confidential – Source Code – Restricted Access Only Material on an encrypted CD(s), DVD(s), hard drive(s), virtual drive(s) or other media. Access to the password(s) or decryption key(s) used to unlock the encrypted media shall be restricted and such password(s) or decryption key(s) shall be stored securely. Upon request, if the Producing Party has a justifiable belief that Highly Confidential – Source Code – Restricted Access Only Material has been improperly disclosed, the Receiving Party shall provide the Producing Party with a list of the persons with access to such password(s) or decryption key(s). The parties may use the free software tool TrueCrypt (www.truecrypt.org, version 7.0) to encrypt Highly Confidential – Source Code – Restricted Access Only Material. Regardless of the encryption tool used, the Receiving Party must keep the Highly Confidential – Source Code – Restricted Access Only Material in an encrypted and inaccessible state whenever possible. For example, if TrueCrypt is used, the Receiving Party shall maintain the Highly Confidential – Source Code – Restricted Access Only Material in a TrueCrypt container / volume, which will ensure that the Highly Confidential – Source Code – Restricted Access Only Material is only decrypted in random-access memory (RAM); additionally, the Receiving Party shall only mount the TrueCrypt volume containing the Highly Confidential – Source Code – Restricted Access Only Material to a drive as needed to review the code; when a review session is over, the volume will be dismounted.

c. Regardless of how a Producing Party produces Highly Confidential – Source Code – Restricted Access Only Material, the Receiving Party shall store any Highly Confidential – Source Code – Restricted Access Only Material in a locked room. Access to the key(s) used to unlock any such room shall be restricted and, upon request if the Producing Party has a justifiable belief that Highly Confidential – Source Code – Restricted Access Only Material has been improperly disclosed, the Receiving Party shall provide the Producing Party with a list of the persons who have had access to such key(s). Any entrance to the locked room must be marked with an "Access Restricted" notice. The Receiving Party shall maintain a log of all persons entering any such room to view Highly Confidential – Source Code – Restricted Access Only Material and shall provide a copy of the log to the Producing Party upon request if the Producing Party has a justifiable belief that Highly Confidential – Source Code – Restricted Access Only Material has been improperly disclosed.

d. Regardless of how a Producing Party produces Highly Confidential – Source Code – Restricted Access Only Material, the Receiving Party may electronically access such Highly Confidential – Source Code – Restricted Access Only Material only from a computer that is not connected to the Internet or a network, that is password-protected and that is kept in a locked room as described in paragraph 5(c). The password(s) used to protect any such computer shall be stored securely and access to such password(s) shall be restricted to the same individuals who have access to the password(s) or decryption key(s) used to unlock encrypted media.

e. The Producing Party may choose to produce Highly Confidential – Source Code – Restricted Access Only Material by producing a computer containing the Highly Confidential – Source Code – Restricted Access Only Material ("Computer Option"). If the Producing Party chooses the Computer Option, the Receiving Party may not electronically transfer the Highly Confidential – Source Code – Restricted Access Only Material from the Computer Option computer to another device. Any Computer Option computer must be equipped with a Windows XP or Windows 7 operating system, at least 100 GB of hard disk storage, at least 2 GB of RAM and a modern processor (e.g., dual-core Intel processor). Additionally, the Producing Party must configure any Computer Option computer to be password-protected as described above. The Producing Party may choose to disable or remove hardware options on or from the Computer Option computer, such as network interface cards, USB ports and optical drives, provided that the Computer Option computer can be adequately used to review the Highly Confidential – Source Code – Restricted Access Only Material stored thereon. The Receiving Party may not alter the hardware configuration of the Computer Option computer without the Producing Party's written consent. If the Computer Option computer does not have a USB port or optical drive enabled, it must install any software (to the extent permitted by law) that the Receiving Party desires prior to producing the Computer Option computer, or else give the Receiving Party its written consent to enable a USB port or optical drive for such purpose. The Receiving Party and Producing Party shall confer regarding any issues with the configuration of a

Computer Option computer and the Producing Party shall not unreasonably withhold its consent to modifications to the Computer Option computer that will improve the Receiving Party's ability to review the Highly Confidential – Source Code – Restricted Access Only Material stored thereon without seriously compromising the security of such Highly Confidential – Source Code – Restricted Access Only Material. Upon termination of this litigation with finality or upon settlement, the Receiving Party must return to the Producing Party any Computer Option computer unless the Producing Party permits its destruction, in which the case the Receiving Party may alternatively ensure that the hard drive of the Computer Option computer is securely erased in a manner agreed to by the Producing Party.

f. The Receiving Party may print limited portions of Highly Confidential – Source Code – Restricted Access Only Material as reasonably necessary to facilitate the Receiving Party's furtherance of its claims and defenses in this case. If Highly Confidential – Source Code – Restricted Access Only Material is stored on a Computer Option computer that is not configured to be used with a printer, the Producing Party shall not unreasonably refuse to produce such limited portions of the Highly Confidential – Source Code – Restricted Access Only Material in accordance with the parties' agreements regarding electronically stored information and Documents originating in electronic format; as an alternative to producing such limited portions, the Producing Party may give the Receiving Party written consent to configure and connect the Computer Option computer to a local computer for the limited purpose of printing such limited portions of the Highly Confidential – Source Code – Restricted Access Only Material, so long as any printouts are stamped with "Highly Confidential – Source Code – Restricted Access Only." Nothing in this Protective Order prevents the parties from including Highly Confidential – Source Code – Restricted Access Only Material in court filings made under seal or from preparing exhibits including Highly Confidential – Source Code – Restricted Access Only Material to be used in expert reports or at depositions, hearings, trial, mediation or other proceedings in this case. Except as otherwise permitted by this Protective Order, the Receiving Party will not electronically transmit any of the Producing Party's Highly Confidential – Source Code – Restricted Access Only Material in any way from the offices of its Outside Counsel. However, nothing in this Protective Order prevents a Receiving Party from making and storing electronic copies of Highly Confidential – Source Code – Restricted Access Only Material on a computer (including a Computer Option computer), provided that in making, storing and accessing such electronic copies the Receiving Party continues to comply with the provisions of this Protective Order. If the original Highly Confidential – Source Code – Restricted Access Only Material is stored on a Computer Option computer whose hardware configuration does not permit data to be transferred to another computer, the Receiving Party must keep any electronic copies of the original Highly Confidential – Source Code – Restricted Access Only Material on the same Computer Option computer unless the Producing Party provides its written consent for the Receiving Party to do otherwise. The Receiving Party shall only make electronic copies of Highly Confidential – Source Code – Restricted Access Only Material to the extent reasonably necessary to facilitate the Receiving Party's furtherance of its claims and defenses in this case. Non-exhaustive examples of permissible reasons for making electronic copies include making copies for back-up purposes or so that a Receiving Party may electronically annotate a copy of the Highly Confidential – Source Code – Restricted Access Only Material.

g. A Receiving Party (apart from the persons identified in paragraph 4(a)) may only transmit or transport Highly Confidential – Source Code – Restricted Access Only Material as follows: (a) if physically lodged or filed with the Court, served upon any Party, or sent to any other person authorized under this Protective Order to receive Highly Confidential – Source Code – Restricted Access Only Material, the Highly Confidential – Source Code – Restricted Access Only Material must be sent (i) in a sealed container via an established overnight, freight, delivery, or messenger service or (ii) via secure FTP to the extent expressly permitted by this Protective Order; (b) if the Highly Confidential – Source Code – Restricted Access Only Material is physically transported for any other purpose, the Receiving Party must retain physical custody and control of the Highly Confidential – Source Code – Restricted Access Only Material at all times and must store it in a locked, secure place. A Receiving Party must notify the Producing Party immediately upon learning that the transported Highly Confidential – Source Code – Restricted Access Only Material did not reach its intended destination. With respect to subparagraphs (5)(g)(a) and

(5)(g)(b), except when being physically lodged or filed with the Court, the Highly Confidential – Source Code – Restricted Access Only Material must be transported on encrypted media.

h. Notwithstanding paragraphs (5)(b) though (g), and to the extent authorized to receive Highly Confidential – Source Code – Restricted Access Only Material, a Receiving Party may store transcripts, recordings and exhibits (including those associated with depositions, trial or other proceedings featuring testimony) designated "Highly Confidential – Source Code – Restricted Access Only" on non-encrypted media and may electronically access them from a computer that is connected to the Internet or a network, provided that access to such transcripts, recordings and exhibits is restricted to a limited number of people or users within the Receiving Party's firm, organization, system, network, etc. by password or by privileges set by an administrator. Nothing in this Protective Order precludes a Receiving Party from storing on non-encrypted media and accessing from a computer that is connected to the Internet or a network any Litigation Material whose portions designated "Highly Confidential – Source Code – Restricted Access Only" have been redacted or otherwise removed.

6. Non-parties producing Documents in the course of this action may also designate Documents as "Confidential" or "Confidential - Attorneys' Eyes Only," subject to the same protections and constraints as the parties to the action. A copy of the Protective Order shall be served along with any subpoena served in connection with this action. All Documents produced by such non-parties shall be treated as "Confidential -

Attorneys' Eyes Only" for a period of 14 days from the date of their production, and during that period any party may designate such Documents as "Confidential" or "Confidential - Attorneys' Eyes Only" pursuant to the terms of the Protective Order.

7. Each person appropriately designated pursuant to paragraph 4(f) to receive Confidential information shall execute a "Written Assurance" in the form attached as Exhibit A. The party or attorney retaining such person may disclose Confidential Documents or the information contained therein to such person no earlier than 10 days after serving on the Producing Party's counsel such executed Written Assurance along with (i) a curriculum vitae of such person, (ii) an identification of any past or present employment or consulting relationship with any party, any related company or any company whose business relates or related to computer networks and an identification of the subject matter of any work performed in the course of such relationship, and (iii) a description of such person's employment or consulting during the past four (4) calendar years, including the name and address of each entity (including natural persons) who employed or used the services of such person and an identification of the subject matter of any work performed in the course of such employment or consulting. If the Producing Party objects in writing to such disclosure within 10 days of such service, no disclosure shall be made until the party seeking disclosure obtains the prior approval of the Court or the objecting party.

8. All depositions or portions of depositions taken in this action that contain trade secret or other confidential information may be designated "Confidential" or "Confidential - Attorneys' Eyes Only" or "Highly Confidential – Source Code –

Restricted Access Only" and thereby obtain the protections accorded other so designated Documents. Confidentiality designations for depositions shall be made either on the record or by written notice to the other party within 14 days of receipt of the transcript. Unless otherwise agreed, depositions shall be treated as "Confidential - Attorneys' Eyes Only" during the 14-day period following receipt of the transcript or, if any material designated "Highly Confidential – Source Code – Restricted Access Only" was discussed during the deposition, then the entire deposition shall be so treated during such 14-day period. The deposition of any witness (or any portion of such deposition) that encompasses Confidential information shall be taken only in the presence of persons who are qualified to have access to such information.

9. Any party who inadvertently fails to identify Documents as "Confidential" or "Confidential - Attorneys' Eyes Only" or "Highly Confidential – Source Code – Restricted Access Only" shall have 14 days from the discovery of its oversight to correct its failure. Such failure shall be corrected by providing written notice of the error and substituted copies of the inadvertently produced Documents. Any party receiving such inadvertently unmarked Documents shall make reasonable efforts to retrieve Documents distributed to persons not entitled to receive Documents with the corrected designation.

10. Any party who inadvertently discloses Documents that are privileged or otherwise immune from discovery shall, promptly upon discovery of such inadvertent disclosure, so advise any Receiving Party and request that the Documents be returned or destroyed. The Receiving Party and its counsel shall take steps consistent with Federal Rule of Evidence 502, either by returning or destroying such inadvertently produced

Documents, including all copies, within 7 days of receiving such a written request. The party returning or destroying such inadvertently produced Documents may thereafter seek re-production of any such Documents as non-privileged, pursuant to applicable law.

11. If a party files a Document containing Confidential information with the Court, it shall do so in compliance with the Electronic Case Filing Procedures for the District of South Dakota. Prior to disclosure at trial or a hearing of materials or information designated “Confidential” or “Confidential - Attorneys’ Eyes Only” or “Highly Confidential – Source Code – Restricted Access Only,” the parties may seek further protections against public disclosure from the Court.

12. Any party may request a change in the designation of any information designated “Confidential,” “Confidential - Attorneys’ Eyes Only” and/or “Highly Confidential – Source Code – Restricted Access Only.” Any such Document shall be treated as designated until the change is completed. If the requested change in designation is not agreed to, the party seeking the change may move the Court for appropriate relief, providing notice to any non-party whose designation of produced Documents as “Confidential” and/or “Confidential - Attorneys’ Eyes Only” in the action may be affected. The party asserting that the material is Confidential shall have the burden of proving that the information in question is within the scope of protection afforded by Fed. R. Civ. P. 26(c).

13. Within 60 days of the termination of this action, including any appeals, each party shall either destroy or return to the opposing party all Documents designated by the opposing party as “Confidential” or “Confidential - Attorneys’ Eyes Only” or

"Highly Confidential – Source Code – Restricted Access Only," and all copies of such Documents, and shall destroy all extracts and/or data taken from such Documents. Each party shall provide a certification as to such return or destruction as within the 60-day period. Attorneys shall be entitled to retain, however, a set of all Documents filed with the Court and all correspondence generated in connection with the action.

14. Any party may apply to the Court for a modification of the Protective Order, and nothing in the Protective Order shall be construed to prevent a party from seeking such further provisions enhancing or limiting confidentiality as may be appropriate.

15. No action taken in accordance with the Protective Order shall be construed as a waiver of any claim or defense in the action or of any position as to discoverability or admissibility of evidence.

16. The obligations imposed by the Protective Order shall survive the Termination of this action. Within 60 days following the expiration of the last period for appeal from any order issued in connection with this action, the parties shall remove any materials designated "Confidential" or "Confidential - Attorneys' Eyes Only" or "Highly Confidential – Source Code – Restricted Access Only" from the office of the Clerk of Court. Following that 60-day period, the Clerk of Court shall destroy any so designated materials.

Dated: ______________

BY THE COURT:

____
ROBERTO A. LANGE
UNITED STATES DISTRICT JUDGE

EXHIBIT A

WRITTEN ASSURANCE

______________________________ declares that:

I reside at ______________________________in the city of ________________, county ________________ , state of _________________________ ;

I am currently employed by ____________________ located at ____________________and my current job title is ___________________________.

I have read and believe I understand the terms of the Protective Order dated _______ , filed in *LodgeNet Interactive Corp. v. Nomadix, Inc.*, Civil Action No. 10-cv-04036-RAL, pending in the United States District Court for the District of South Dakota. I agree to comply with and be bound by the provisions of the Protective Order. In particular, if Protected Technical Material is disclosed to me, I will not, until two (2) calendar years after the termination of this action (including any appeals), on behalf of a patent applicant or patentee, prepare and/or amend any patent applications of any kind, draft and/or amend patent claims of any kind (including claims that are the subject of reissue or reexamination proceedings), supervise such activities, or consult on such activities whenever such patent applications or patent claims relate to (1) the patents-in-suit or contain claims that it is reasonably likely may be asserted against the Producing Party in this action or any other action; and relate to (2) charging for, providing or controlling access to computer networks, or to network devices involved in charging for, providing or controlling access to computer networks.

I understand that any violation of the Protective Order may subject me to sanctions by the Court.

I shall not divulge any documents, or copies of documents, designated "Confidential," "Confidential - Attorneys' Eyes Only," or "Highly Confidential – Source Code – Restricted Access Only" obtained pursuant to such Protective Order, or the contents of such documents, to any person other than those specifically authorized by the Protective Order. I shall not copy or use such documents except for the purposes of this action and pursuant to the terms of the Protective Order.

As soon as practical, but no later than 30 days after final termination of this action, I shall return to the attorney from whom I have received them, any documents in my possession designated "Confidential," "Confidential - Attorneys' Eyes Only," "Highly Confidential – Source Code – Restricted Access Only," and all copies, excerpts, summaries, notes, digests, abstracts, and indices relating to such documents.

I submit myself to the jurisdiction of the United States District Court for the District of South Dakota for the purpose of enforcing or otherwise providing relief relating to the Protective Order. I declare under penalty of perjury that the foregoing is true and correct.

Executed on:

______________________________	______________________________
(Date)	(Signature)